NASA/TM—2002-211140

Application of Mobile Router to Military Communications

David H. Stewart
Verizon, Cleveland, Ohio

William D. Ivancic
Glenn Research Center, Cleveland, Ohio

Terry L. Bell
Lockheed Martin Global Telecommunications, Cleveland, Ohio

Brian A. Kachmar
Analex Corporation, Brook Park, Ohio

Dan Shell and Kent Leung
Cisco Systems, San Jose, California

January 2002

The NASA STI Program Office . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the Lead Center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA's counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that complement the STI Program Office's diverse offerings include creating custom thesauri, building customized data bases, organizing and publishing research results . . . even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at ***http://www.sti.nasa.gov***

- E-mail your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA Access Help Desk at 301–621–0134

- Telephone the NASA Access Help Desk at 301–621–0390

- Write to:
  NASA Access Help Desk
  NASA Center for AeroSpace Information
  7121 Standard Drive
  Hanover, MD 21076

NASA/TM—2002-211140

Application of Mobile Router to Military Communications

David H. Stewart
Verizon, Cleveland, Ohio

William D. Ivancic
Glenn Research Center, Cleveland, Ohio

Terry L. Bell
Lockheed Martin Global Telecommunications, Cleveland, Ohio

Brian A. Kachmar
Analex Corporation, Brook Park, Ohio

Dan Shell and Kent Leung
Cisco Systems, San Jose, California

Prepared for the
MILCOM 2001
cosponsored by the IEEE, IEEE Communications Society, and AFCEA
Vienna, Virginia, October 28–31, 2001

National Aeronautics and
Space Administration

Glenn Research Center

January 2002

Available from

NASA Center for Aerospace Information
7121 Standard Drive
Hanover, MD 21076

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22100

Available electronically at http://gltrs.grc.nasa.gov/GLTRS

APPLICATION OF MOBILE ROUTER TO MILITARY COMMUNICATIONS

David H. Stewart
Verizon
Cleveland, Ohio 44135

William D. Ivancic
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

Terry L. Bell
Lockheed Martin Global Telecommunications
Cleveland, Ohio 44135

Brian A. Kachmar
Analex Corporation
Brook Park, Ohio 44142

Dan Shell and Kent Leung
Cisco Systems
San Jose, California 95135

ABSTRACT

Cisco Systems and NASA Glenn Research Center under a NASA Space Act Agreement have been performing joint networking research to apply Internet technologies and protocols to space-based communications. During this time, Cisco Systems developed the mobile-router which NASA and Cisco jointly tested. The early field trials of this technology have been successfully completed.

The mobile-router is software code that resides in a network router. A Mobile-Router allows entire networks to roam while maintaining connectivity to the Internet. This router code is pertinent to a myriad of applications for both the government and commercial sectors. This technology will be applied to the wireless battlefield. NASA and the DoD will utilize this technology for near-planetary observation and sensing spacecraft. It is the enabling technology for communication via the Internet or Intranets to aircraft. Information such as weather, air traffic control, voice and video can be easily and inexpensively transmitted to the aircraft using Internet protocols. The mobile router can be incorporated into emergency vehicles particularly ambulances and life-flight aircraft to provide real-time connectivity back to the hospital and healthcare experts. Commercial applications include entertainment services, IP telephone, and Internet connectivity for cruise ships, commercial shipping, tour busses, aircraft, and eventually cars.

This paper will briefly describe the mobile router operation. An upcoming wide area network field test with application to U.S. Coast Guard communications will be described. The paper will also highlight military and government networks that will benefit from the deployment of mobile router and the associated applications.

INTRODUCTION

Cisco Systems and NASA Glenn Research Center under a NASA Space Act Agreement have been performing joint networking research to apply Internet technologies and protocols to aeronautic and space-based communications. Cisco Systems developed the mobile-router during this time and provided the technology for both the commercial and government markets. The technology was provided to NASA for evaluation of its applicability to NASA's aeronautic and space-based networks. By performing joint testing of the mobile router, NASA was able to provide input as to the applications and requirements. Cisco was then able to modify the code where appropriate to address those needs and requirements. This paper will describe mobile-IP, the mobile router, the test network and additional testing scenarios that are presently underway.

MOBILE-IP OVERVIEW

Mobile-ip [Ref. 1] is a routing protocol that allows hosts (and networks) to seamlessly "roam" among various IP subnetworks. This is essential in many wireless networks. Mobile-ip can also be useful in wireless networks where the mobile-node's point of attachment to the network is changing due to varying conditions in the wireless medium, even if the mobile-node is not physically moving. Mobile-IP can also be used in a wired network where the mobile-node simply wishes to maintain its network identity as the mobile-node is always contacted through association of its home IP address.

There are three basic elements in mobile-ip, the home-agent, the foreign-agent and the mobile-node.

"The Home-agent (HA) is a router on a mobile-node's home network that tunnels datagrams for delivery to the mobile-node when it is away from home, and maintains current location information for the mobile-node. The home-agent is the gateway to the mobile-node (i.e., all traffic destined for the mobile-node must pass through the home-agent).

The Foreign-agent (FA) is a router on a remote network that provides routing services to a registered mobile-node. The foreign-agent receives datagrams from the home-agent via an IP tunnel, which are then forwarded to the mobile-node. For datagrams sent by a registered mobile-node, the foreign-agent serves as a default router.

The Mobile-node (MN) is a host or router that changes its point of attachment from one network or subnetwork to another. A mobile-node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (constant) IP address, assuming link-layer connectivity to a point of attachment is available." [Ref. 1]

A mobile-node first determines if it is attached to its home network or a foreign network using ICMP (Internet Control Message Protocol) Router Discover messages. If it is attached to a foreign network, the mobile-node will determine if a foreign-agent is available. If so, the mobile-node registers with the home-agent via the foreign-agent, and a unidirectional IP tunnel[1] is established from the home-agent to the foreign-agent. The home-agent will now encapsulate all packets destined for the mobile-node and tunnel them to the foreign-agent. The foreign-agent de-encapsulates the packets and forwards them on to the mobile-node. Standard IP routing is used to deliver datagrams sent by the mobile-node, with the foreign-agent as the mobile-node's default router.

Figure 1 depicts mobile-ip operation when the mobile-node is a single host. In this scenario, the corresponding node request information from the mobile-node. The request first is sent to the mobile-node's home IP address via the Internet. Thus, the request goes to the home-agent. The home-agent encapsulates the request in a second ip packet and tunnels that request through the Internet to the foreign-agent. The foreign-agent de-encapsulates the request and passes it on to the mobile-node via the care-of-address. Once the mobile-node receives the request, the mobile-node sends a reply to the Corresponding Node through normal IP routing. The reply goes to the foreign-agent, which passes it on to the Corresponding Node via the Internet.

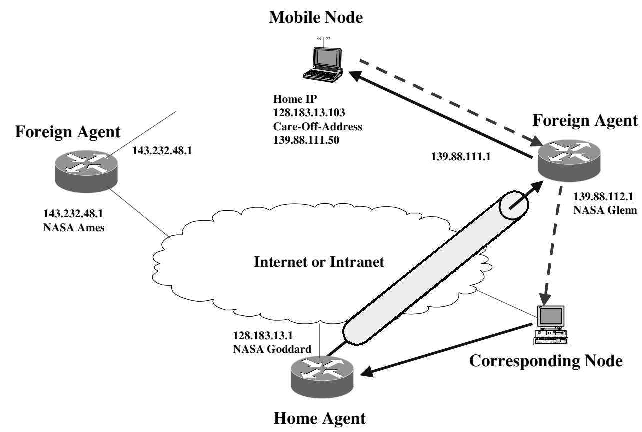

Figure 1 - Mobile-ip Tunneling

MOBILE-ROUTER OVERVIEW

Mobile-router is software that resides in a network router. It is part of the mobile-ip standards specification (RFC 2002). A mobile-router (MR) allows an entire network to roam (Future references to this roaming network will be designated as "mobile-network"). Hence, a device connected to the mobile-router does not need to support mobile-ip since the mobile-router is providing the roaming capabilities.

Cisco Systems has recently developed mobile-router code. NASA Glenn and Cisco, through a Space Act Agreement, have been performing joint research and validation tests on this code, which will become part of Cisco Systems IOS (Internetworking Operating System) in September 2001. The current version of the mobile-router IOS only supports a stub network, but is scheduled to support dynamic routing on the mobile-network in later releases.

The mobile-router IOS allows a router to be a mobile-node. The main difference between mobile host and mobile-router operations is that a 2nd tunnel is established. This tunnel is between the home agent and the mobile router, and is used to forward packets destined for the hosts residing on the mobile-network. Once the mobile-router has registered with the home-agent, the

[1] Tunneling is a technique that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

home-agent will inject the mobile-router's networks into the home-agent's routing table. Thus, the home-agent will not only forward packets destined to the mobile-router (mobile-node), but will forward packets destined to the hosts connected to the mobile-network. This implementation is fully compliant to the RFC 2002 standard.

Figure 2 depicts mobile-ip operation when the mobile-node is a network (i.e., the mobile-node is a mobile-router). The operation is nearly identical to that of mobile-ip for a single host, except that two tunnels are established: one between the home-agent and foreign-agent (tunnel-1) and one between the home-agent and mobile-router (tunnel-0). The function of tunnel-1 is to route the packets destined for the mobile-router to the foreign-agent. The foreign agent then forwards the packets to the interface that mobile-router is attached to. The 2nd tunnel (tunnel-0) is to forward the packets destined for the mobile-network to the mobile-router. The mobile-router then routes these packets to its appropriate interface.

To instill on the reader how this operation transpires let's track a ping from the corresponding node (CN) to host 'H' on mobile-router's LAN interface (mobile-network) shown in figure 2. The CN initiates a ping with 'H' as the destination address. In the home-agent, the mobile-network is defined as a directly connected virtual network,[2] so to the rest of the world 'H' appears to be on a subnet directly connected to the home-agent. Therefore when the ping reaches the internet it is routed to the home-agent.

After receiving the packet, home-agent performs a double encapsulation. Since the final destination of the packet is on the mobile-routers LAN, the first encapsulation has mobile-router's address as the destination. The home agent then encapsulates the packet a second time with the foreign-agent as the destination. The encapsulated packet is then routed to the foreign-agent. The foreign-agent performs the first de-encapsulation, then forwards the packet destined for the mobile-router out the interface that mobile-router is attached to. The mobile-router performs the second de-encapsulation, then routes the packet to the subnet that host 'H' resides on.

After receiving the ping, host 'H' responds with an acknowledgement (Ack) destined for the CN. The Ack is sent to the mobile-router. The mobile-router forwards the

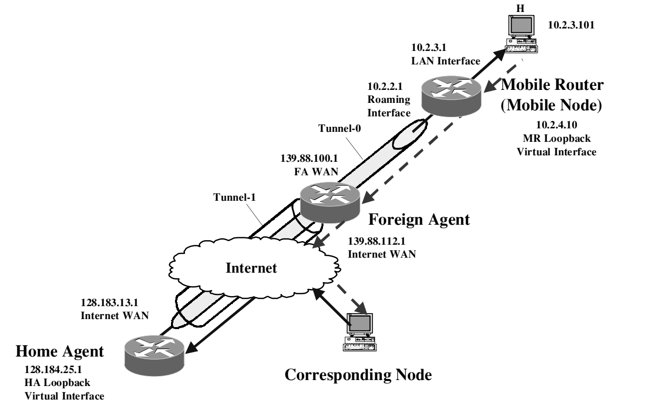

Figure 2 – Mobile-Router Tunneling

Ack to the active foreign-agent, where it is routed as a typical IP packet to the corresponding node.

As the mobile-router moves, it will register with its home-agent on its whereabouts via various foreign-agents. Thus, a mobile-router is a mobile-node; however, the node is a network rather than a single host.

MOBILE-ROUTER FEATURES

The mobile-router has a number of features that make it applicable to a variety of networks and applications.

The mobile-router can have multiple roaming interfaces.[3] This allows for connection to a variety of different wired and wireless links. One example would be for a mobile-router residing on an aircraft and having three different roaming WAN interfaces and two non-roaming LAN interfaces. One LAN may be for aircraft operations (flight information services, air traffic control, weather, etc.) while the second LAN is reserved for tactical data. One roaming interface may be a 100Base-T interface for a wired connection while on the ground. A second roaming interface may be connected to a VDL (VHF Data Link) antenna. The third roaming interface may be connected to a satellite antenna.

The mobile-router can perform smooth handoffs using preferred path routing or priority routing. The mobile-router maintains a list of available foreign-agents, up to one per roaming interface. From this list mobile-router determines which foreign-agent to use for registration to the home-agent. Consider the aircraft example: The VDL link may be active during take-off. Once in flight, both

[2] The virtual-network defined in the home-agent must encompass the IP addresses assigned to mobile-router along with the entire mobile-network.

[3] The mobile-router has two types of interfaces a roaming and a LAN (aka mobile LAN). The roaming interfaces have the ability to dock to a foreign agent.

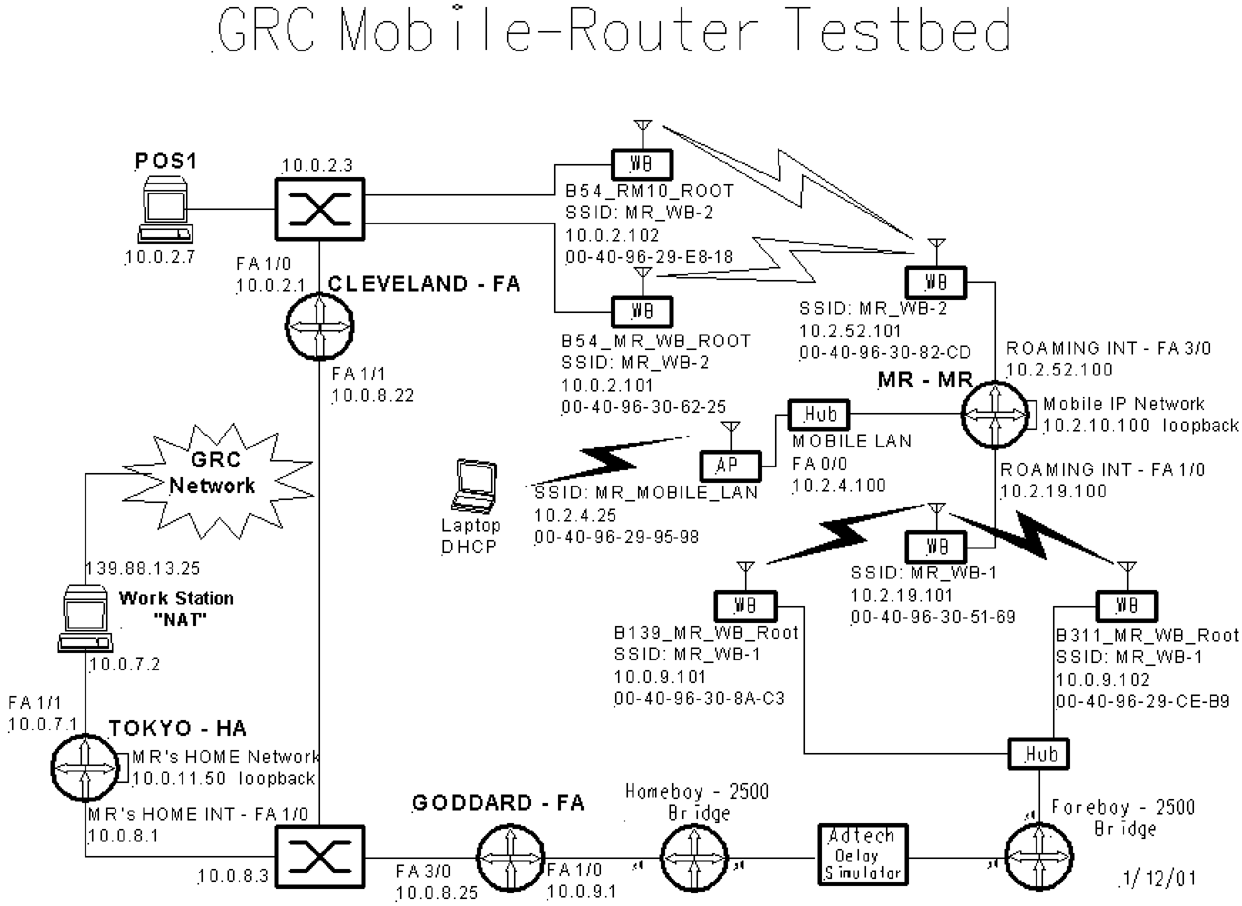

Figure 3 – GRC Mobile-Router Testbed

the VDL link and the satellite link may be available. The preferred path may be the satellite link assuming greater bandwidth. In this case, the routing will automatically switch the active link from the VDL to the satellite link. If both links are up and the satellite link goes down, the routing will automatically revert back to the VDL link. If for some reason, one would prefer the VDL link be utilized (for whatever reason—cost, delay, etc.), the VDL link can be set to have a higher priority than the satellite link. Thus, when both links are available, the routing would be via the path with highest priority.

One feature of the home-agent is that it can be configured for hot-standby. This is significant since, if the home-agent were to experience a catastrophic failure, connectivity to all mobile-routers serviced by this home-agent would be lost. Hot-standby was demonstrated by pulling the power plug on the active home-agent and noting restoration time for the hot-standby home agent to come online. Restoration was nearly instantaneous, and totally transparent to a client on the mobile-network.

The mobile-routing protocols perform well in long delay environments. Testing was done by inserting a satellite delay simulator (see figure 3) between the mobile-router and one of the foreign-agents. Then while transferring data and initiating switching between preferred and non-preferred paths, the link delay was increased until the mobile-router would fail to register to the home-agent due to the timestamp being out of bounds in the MD5 authentication. The failure occurred when the RTT from the home agent to the mobile-router was increased from 3 to 4 seconds. This indicates that the mobile-router is capable of working over links with round trip time delays in excess of 3 seconds, which is far greater than a double, geostationary satellite hop.

As of July 2001, the following areas were still being addressed: IPSec[4] (Internet Protocol Security) between the foreign-agent and mobile-router, multicasting, and unidirectional link routing (UDLR).[5] Currently, MD5

[4] The IPSec protocol provides secure, interoperable communication across a network, transparent to the application.
[5] UDLR is describes a mechanism to emulate bi-directional connectivity between nodes that are directly connected by a unidirectional link.

hashing is utilized between the mobile-router and home-agent for authentication, and security can also be implemented between the foreign-agent and home-agent via IPSec and/or via establishment of access lists in the home-agent.

TEST NETWORK – EARLY FIELD TRIALS

In order to test the mobile-router in a relevant environment, a wired and wireless mobile testbed was developed at NASA Glenn. Figure 3, depicts the network configuration of that testbed. We have four mobile-ip enabled routers: one home-agent, two foreign agents and one mobile-router. Two additional routers reside between the mobile-router and one foreign agent (Goddard). These routers are configured to be bridges and provide an interface for a satellite channel emulator. The satellite emulator is an Adtech SX/14 and provides both delay and error capability. We have used this unit in the mobile router testing to generate delay over on duplex path. A linux workstation is connected to the home-agent and acts as a network address translator (NAT) in order to allow routing from the 10.x.x.x network to the NASA Glenn network for demonstrations purposes.

The mobile-router resides in a half-rack roll-around cabinet [Figure 4] such that we can place this unit in the laboratory or on a van. The router is a Cisco 3640 with one Voice over IP interface card and 3 ethernet NICs. Two of the ethernet interfaces are configured as roaming interfaces, and perform the task of agent-discovery via a wired or wireless connection to a foreign-agent. The third ethernet interface is a standard LAN, referred to as the mobile-LAN, since it moves with the mobile-router. The mobile-LAN also has wireless capabilities (access-point) as well as a wired hub in order to easily add application and test computers to the network. For this reason, DHCP (RFC 1533—dynamic host control protocol) is also running on the mobile-LAN. The Voice over IP interface card provides the mobile-router the ability to support telephone conversations while in transit. An uninterruptible power supply (UPS) allows for 1 to 2 hours of mobile operation. In addition, the UPS cleans up the power provided by a generator in the mobile-van.

Figure 4 - Mobile-Router Rack

There are four 802.11 wireless bridges deployed for WAN connections, two for each foreign agent. One of the wireless bridge antennas is located in the laboratory and is used when the mobile-router is being tested there. The other three wireless bridges are deployed on various buildings throughout the Glenn Research Center. Figure 5 shows a map of the antenna locations and a rough coverage map. One wireless antenna connects to foreign-agent Cleveland that has no delay. The second two antennas are connected to foreign-agent Goddard and have the programmable delay unit in the path between the foreign agent and the home-agent. All connections are fiber-repeated back to the laboratory in order to keep the beta testing off the production network. However, plans are to move to the production network as soon as performance testing is complete.

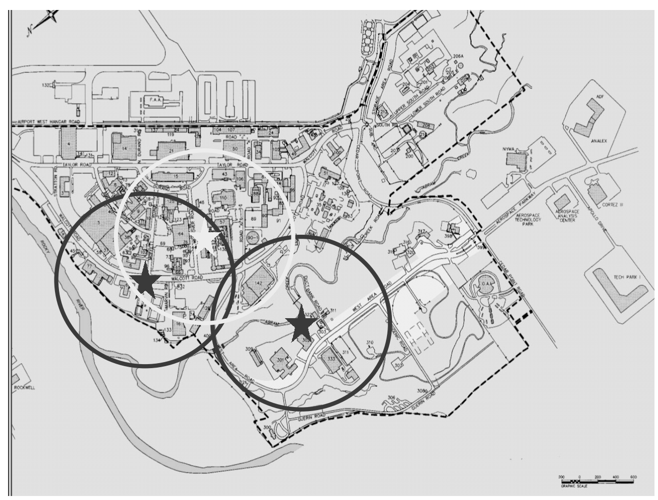

Figure 5 - Wireless Ethernet Antenna Coverage

The antenna sights were picked such that we would have simultaneous coverage at some times thereby enabling testing of smooth handoffs and preferred path operation. The darker circles in figure 5, are the wireless bridges with the simulated delay. The lighter circle's wireless bridge has no delay and is configured as the preferred path. With this configuration, the mobile-router van, driven from one end of the Glenn Research Center's campus to the other starts the trip connected to a delayed, non-preferred path (simulated satellite link) switches to the preferred path, then switches back to yet a different delayed, non-preferred path (simulated satellite link). The transition from non-preferred to preferred-path is almost transparent to the end-user connected to the mobile-router, but there is a 20 to 30 second loss of connection in the transition from preferred to non-preferred path.

The difference in switch times is due to the mechanics of how each event is handled. Switching from a non-preferred to a preferred path is initiated by the discovery of a new foreign-agent on a higher priority interface. When this occurs the mobile-router immediately re-registers through the new foreign-agent and the home-agent updates the routing table. The mobile-router maintains the connectivity via the non-preferred path until this process is complete. Thus mobile-router never loses connectivity during this process, just changes the data path.

On the other hand, switching from a preferred to non-preferred path is the result of a broken pipe on the preferred path. Unless the broken pipe causes an interface to go down the mobile-router is unaware of the loss of connectivity until either the registration lifetime or the FA advertisement timer expires. During this period mobile–router is completely isolated. How fast the mobile-router reacts depends on the configuration of the registration lifetime and advertisement timers, and the location of the break in the pipe.

Figure 6 shows the various antennas deployed throughout the Glenn Research Center and on the mobile-router test van. Dipole antennas are used on the building to provide omni-directional coverage as shown in figure 5. The mobile-router van is equipped with both a yagi and a dipole antenna for each wireless bridge (one bridge per roaming interface). The yagis provide greater gain, but are directional. The yagi antennas enable us to test at farther distances if we wish, or to restrict coverage and force handoffs and loss of signal by positioning the yagi antenna so that it points away form the reciprocal signal.

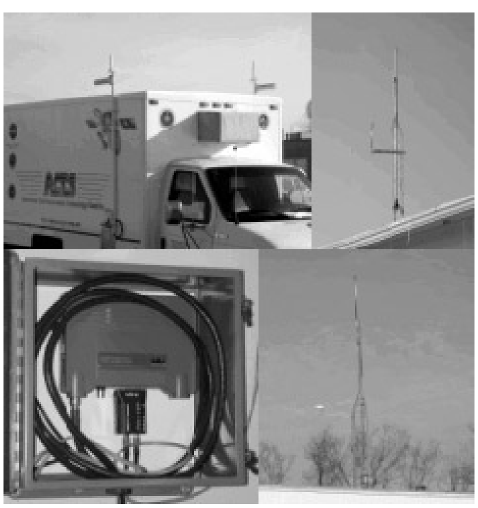

Figure 6 - Picture of Van and Site Antennas

Using the outdoor mobile testbed we have demonstrated the mobile-router functionality via live demonstrations. These live demonstrations validated the general mobile routing algorithms including preferred path. The mobile-router was able to perform with round trip time delays of up to 3 seconds (1.5 seconds in each link). Some of the applications we demonstrated included: email transfers, Web browsing, voice over IP (VOIP), ftp file transfers, secure shell and telnet.

UPCOMING FIELD TESTS

Additional testing in a real life application has been planned. NASA in partnership with Cisco Systems, Ball Aerospace & Technologies Corp., L3 Communications and the U.S. Coast Guard 9th District are making preparations to deploy a mobile-router in the Neah Bay, an ice-cutter stationed in the great lakes region. The goal of the mobile router will be to provide network connectivity to the crew of the Neah Bay, while on their tour of duty. The network connectivity will support Voice-over IP (VoIP), Web Browsing, and online log entry. Presently network connectivity is only available at the Neah Bays homeport of Cleveland via a terrestrial link.

Contributions to this field test are as follows:

- Cisco Systems is supplying the networking equipment.
- Ball Aerospace is supplying an Airlink® antenna system and coordinating the satellite time.
- L3 Communications will supply a 2.4 Ghz tracking antenna that supports 802.11 wireless equipment and is designed for marine use.
- The U.S. Coast Guard will supply a 140’ ice-cutter (Neah Bay).
- NASA Glenn Research Center will provide engineering and labor support for design, implementation and testing.

Figure 7, depicts the network topology of the mobile-router system to be deployed. The implementation will occur in 3 steps. First, a foreign-agent and 2 wireless bridges will be installed at the Cleveland Federal Building. The 2 wireless bridges will each have its own bi-lateral amplifier[6] connected to a 20 dBi gain panel antenna, which will be mounted on top of the Federal Building. The antennas have an elevation of

[6] The bi-lateral amplifier serves two purposes: 1) Amplify the receive signal to eliminate the effects of transmission line loss on the receive side. 2) Increase the transmit power to just under 4 watts ERP to provide maximum range, while maintaining the FCC regulations on the implementation of part 15 devices.

approximately 450' above Lake Erie. The Neah Bay will be outfitted with a mobile-router and 2 wireless bridges. These wireless bridges will also have bi-lateral amplifiers, but will have 2 different antenna systems. The first antenna will be 8 dBi gain dipole mounted on the mast of the Neah Bay. The second will be a 15 dBi tracking antenna designed for marine use by L3 Communications. Two types of antenna are to be used to provide redundancy in case of failure of a bi-lateral amplifier or antenna. Another reason for the second wireless system is to provide a secondary path for testing the mobile-router transition between links, prior to the completion of step 2, of this implementation. The home-agent will reside at the Coast Guard's network operations center.

In Step 2, Ball Aerospace and Technologies Corp. will provide and install their Airlink® High Gain Antenna System on Neah Bay. This system designed to be used on an aircraft is composed of two L-Band electronically steerable phased arrays. This system will provide 2 multiplexed 64 kbps channels delivering full ISDN-2B (128 kbps) service using Inmarsat's Aero H/H+ system. The terrestrial downlink will be at Comsat's ground station in Southbury Connecticut. A foreign-agent[7] must also be located at the satellite ground terminal.

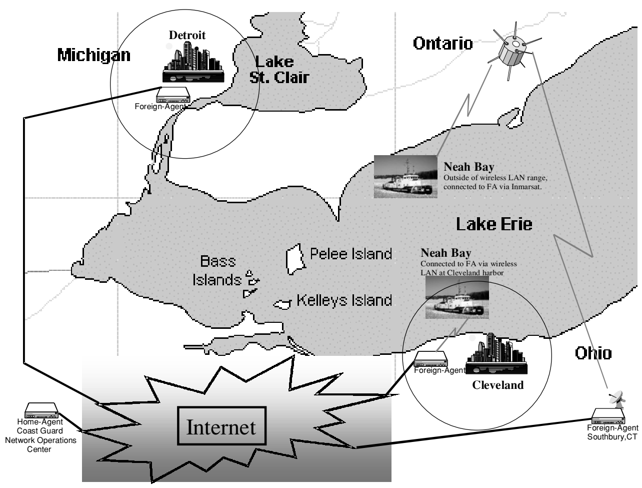

Figure 7

The 3rd and final step of this field test is to deploy wireless bridges at Neah Bay's port in Detroit. The deployment of this equipment will be very similar to that in Cleveland, although it is unlikely that such an ideal antenna site will also be available in Detroit.

After the completion of the 3rd step the system should perform in the following manner. The Neah Bay starts out from her homeport (Cleveland) and the mobile router is connected via the wireless bridges (preferred-path) on the Cleveland Federal Building. This will be considered the preferred-path, since the bandwidth will be higher and the cost cheaper than the path over the satellite. As the Neah Bay steams out into the lake connectivity to the Cleveland Federal Building will fade at this time mobile-router will switch to the satellite connection (non-preferred-path). The mobile-router will maintain registration through the satellite, until the Neah Bay steams into range of the wireless bridges deployed in Detroit. At which time the mobile-router will recognize the Detroit wireless bridges as the preferred-path[8].

MILITARY APPLICATIONS

One of the main advantages of deploying mobile-router technology in a military field application would be the ability for rapid infrastructure deployment. For example, a Battle Group would consist of at least one Mobile Command Post (MCP) that would house a router configured as a foreign-agent, and would have a data-link back to the home-agent at the Battle Group Command Center (BGCC). All other units in the Battle Group would be equipped with mobile-routers. Prior to initial deployment of the Battle Group the MCP's foreign-agent would be configured with the fixed IP address needed to connect to the BGCC's network. After network connectivity is established between the MCP and BGCC, all mobile-routers in the field units would register with the home-agent via the foreign agent in the MCP. The registrations will occur almost instantaneously with no operator intervention what so ever. Unlike a conventional router the mobile-router is a "Set and Forget" technology, which means a technician does not need to reconfigure these devices with every network change. In the event that this Battle Group is relocated, only the foreign-agent of the MCP would have to be reconfigured to connect to the new BGCC. This will greatly decrease the time needed to reconfigure a network. Connectivity to all units can be verified on the foreign-agent's console port.

Figure 8, shows a possible scenario for mobile-router deployment in a military application. The Intelligence Control Center would reside most likely somewhere in the continental United States. This center would gather satellite surveillance images and other tactical data, then forward all intelligence to BGCC. The BGCC would then provide that intelligence to field units via a communication link through an Unmanned Aerial Vehicle

[7] Due to the nature of the mobile-router's agent-discovery process the mobile-router must be on the same wire (0 hop count) as the foreign-agents advertising interface.

[8] Preferred-path is the most desired path that mobile-router has available at any given time, and is determined based on criteria configured in the mobile-router.

(UAV) or the Airborne Warning and Control System (AWACS). The AWACS would also provide tactical data to both the BGCC and the field units.

The home-agent along with its hot-standby backup unit would be deployed at the BGCC. The foreign-agents could be deployed in the UAV and the MCP. While the mobile-routers are deployed in the field units, in this case Armored Fighting Vehicles (a.k.a. Tanks).

When first deployed all field units would be in close proximity to the MCP, as in the case of field unit T-1 in figure 8. The mobile-router in this field unit would have discovered 2 foreign-agents available (UAV & MCP) for registering to the home-agent. The registration would occur through the MCP, since it was configured to be the preferred-path (higher priority link). In the case of unit T-2, communications via the preferred-path has been lost due to a blocked line of sight, therefore mobile-router automatically re-established network connectivity through the foreign-agent on the UAV. The mobile-router on T-2 will immediately switch back to the preferred-path as soon as the communications link is re-established.

The example in figure 9 is an extension of that in figure 8. The network is deployed the same, but multiple battle groups have been added to demonstrate the mobile-router's flexibility. Lets start with the initial deployment again from the networking point of view. All routers from the home-agent to the foreign-agents will have to have fixed addresses. This would include the Intelligence Control Center, the Battle Group Command Center, the UAVs and the Mobile Command Posts in the field (The UAVs and MCPs would house foreign-agents). The remaining field and support units would each be equipped with a mobile-router, which can connect to the foreign-agents dynamically. It is assumed that the mobile-router in a field unit is configured so that it's preferred path is the link back to the mobile command post of the group that it belongs to.

Now, as the Battle Groups engage the mobile-routers will reregister to the appropriate FA as needed. For example, Battle Group B is ordered to have half its complement perform a scouting patrol, and the other half fall in to support Battle Group A. Assuming the MCP accompanies the scouting patrol, the mobile-routers in the units that join Battle Group A will reregister through Battle Group A's MCP. The units on the scouting patrol remained registered via Battle Group B's MCP, but during the patrol the MCP was disabled. Now the mobile-routers reregister via the foreign agents in the UAVs. This would all occur without operator intervention.

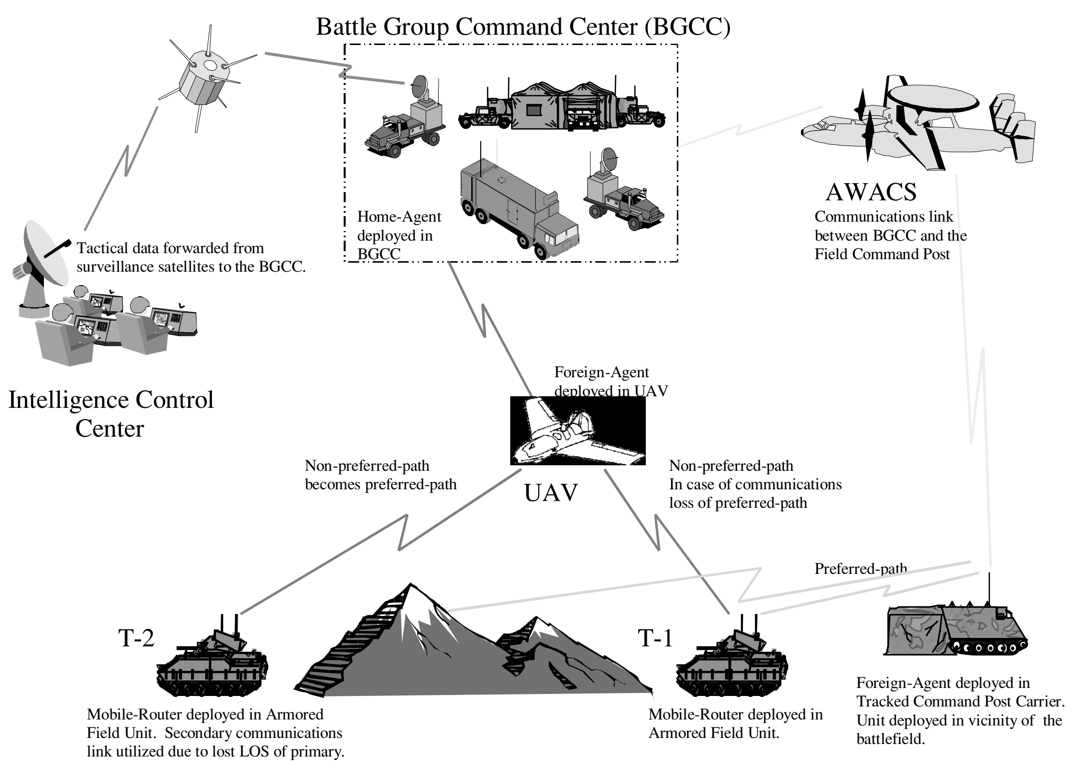

Figure 8

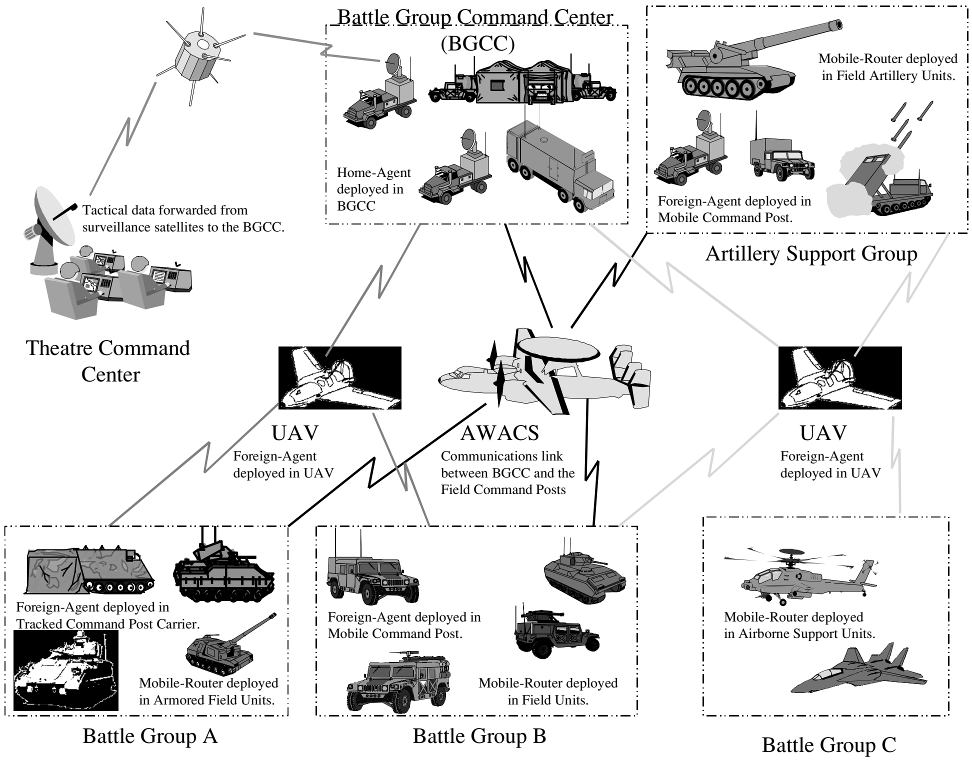

Figure 9

SUMMARY

Mobile-router technology is pertinent to a myriad of applications for both the government and commercial sectors. This technology will be applied to the wireless battlefield. NASA and the DoD will utilize this technology for near-planetary observation and sensing spacecraft. It is the enabling technology for communication via the Internet or Intranets to aircraft. Information such as weather, air traffic control, voice and video can be easily and inexpensively transmitted to the aircraft using Internet protocols. The mobile-router will be incorporated into emergency vehicles–particularly ambulances and life-flight aircraft to provide real-time connectivity back to the hospital and healthcare experts. Commercial applications include entertainment services, IP telephone, and Internet connectivity for cruise ships, commercial shipping, tour busses, aircraft, and eventually cars.

The MR enables communication between military groups in a dynamic environment. Without such a technology, IP communications would be impractical due to the requirement of continuous manual reconfiguration of network-connected devices.

Some of the key features of mobile-router are:

- Mobile-router enables Internet connections from many types of mobile platforms.
- Mobile-router allows for Networks in Motion™.
- Mobile-router is software. Any Cisco Router (model 2600 or better) can be made into a mobile-router by upgrading the IOS.
- MR is set and forget. Configuration only needs to be done once.
- Preferred path can be set by bandwidth or priority.
- Mobile-router has already implemented many IPSec features.
- Dual hot-standby home-agents for mobile-router capability has been demonstrate.
- Mobile-router is the enabling technology for numerous NASA programs and will be highly utilized in the aeronautics arena as well as for low-Earth-orbiting (LEO) Earth observation science (EOS) platforms.

REFERENCES

[1] C. Perkins, RFC 2002 October 1996.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	January 2002	Technical Memorandum

4. TITLE AND SUBTITLE

Application of Mobile Router to Military Communications

5. FUNDING NUMBERS

WU–322–20–2A–00

6. AUTHOR(S)

David H. Stewart, William D. Ivancic, Terry L. Bell,
Brian A. Kachmar, Dan Shell, and Kent Leung

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
John H. Glenn Research Center at Lewis Field
Cleveland, Ohio 44135–3191

8. PERFORMING ORGANIZATION REPORT NUMBER

E–12995

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546–0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

NASA TM—2002-211140

11. SUPPLEMENTARY NOTES

Prepared for the MILCOM 2001 cosponsored by the IEEE, IEEE Communications Society, and AFCEA, Vienna, Virginia, October 28–31, 2001. David H. Stewart, Verizon, 21000 Brookpark Road, Cleveland, Ohio 44135; William D. Ivancic, NASA Glenn Research Center; Terry L. Bell, Lockheed Martin Global Telecommunications, 21000 Brookpark Road, Cleveland, Ohio 44135; Brian A. Kachmar, Analex Corporation, 3001 Aerospace Parkway, Brook Park, Ohio 44142; Dan Shell and Kent Leung, Cisco Systems, 170 W. Tasman Drive, San Jose, California 95135. Responsible person, William D. Ivancic, organization code 5610, 216–433–3494.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Categories: 04, 17, 32 and 62 Distribution: Nonstandard

Available electronically at http://gltrs.grc.nasa.gov/GLTRS
This publication is available from the NASA Center for AeroSpace Information, 301–621–0390.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 words)***

Cisco Systems and NASA Glenn Research Center under a NASA Space Act Agreement have been performing joint networking research to apply Internet technologies and protocols to space-based communications. During this time, Cisco Systems developed the mobile-router which NASA and Cisco jointly tested. The early field trials of this technology have been successfully completed. The mobile-router is software code that resides in a network router. A Mobile-Router allows entire networks to roam while maintaining connectivity to the Internet. This router code is pertinent to a myriad of applications for both the government and commercial sectors. This technology will be applied to the wireless battlefield. NASA and the DoD will utilize this technology for near-planetary observation and sensing spacecraft. It is the enabling technology for communication via the Internet or Intranets to aircraft. Information such as weather, air traffic control, voice and video can be easily and inexpensively transmitted to the aircraft using Internet protocols. The mobile router can be incorporated into emergency vehicles particularly ambulances and life-flight aircraft to provide real-time connectivity back to the hospital and healthcare experts. Commercial applications include entertainment services, IP telephone, and Internet connectivity for cruise ships, commercial shipping, tour busses, aircraft, and eventually cars. This paper will briefly describe the mobile router operation. An upcoming wide area network field test with application to U.S. Coast Guard communications will be described. The paper will also highlight military and government networks that will benefit from the deployment of mobile router and the associated applications.

14. SUBJECT TERMS

Protocol; Satellite

15. NUMBER OF PAGES

15

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	